Vorwort

Ziel des Buches ist eine Darstellung der elementaren Zahlentheorie von der einfachen Teilbarkeits-Lehre über die Theorie der quadratischen Reste bis zu den Anfangsgründen der quadratischen Zahlkörper, wie Einheiten reell-quadratischer Zahlkörper und die Klassengruppe imaginär-quadratischer Zahlkörper. Daneben soll auch die Untersuchung spezieller Zahlen, wie der Fibonacci-Zahlen sowie der Fermat'schen und Mersenne'schen Primzahlen nicht zu kurz kommen. Dabei wird einerseits versucht, durch Beleuchtung des algebraischen Hintergrunds zu einem vertieften Verständnis der Aussagen zu gelangen; andrerseits wird immer auch ein algorithmischer Standpunkt eingenommen. Dieser gibt sich nicht mit reinen Existenzsätzen zufrieden, sondern fragt stets auch, wie man gesuchte existierende Objekte (etwa die Primfaktor-Zerlegung einer natürlichen Zahl oder eine Primitivwurzel modulo einer Primzahl) effizient konstruieren kann.

Die algorithmische Zahlentheorie kann auf eine lange Tradition zurückblicken, gehören doch zwei der ältesten Algorithmen der Mathematik, nämlich der euklidische Algorithmus und das Sieb des Eratosthenes, zur Zahlentheorie. Auch die über 300 Jahre alte Theorie der Kettenbrüche hatte von Anfang an auch einen algorithmischen Aspekt (etwa zur Lösung der Pell'schen Gleichung). Zu zwei Grundproblemen der algorithmischen Zahlentheorie (die heute u.a. in der Kryptographie und für die Computer-Sicherheit praxis-relevant geworden sind) schreibt Gauß in Art. 329 seiner Disquisitiones Arithmeticae (zitiert nach der deutschen Übersetzung von Maser, 1889):

"Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. . . . ; ausserdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen."

Die Hilfsmittel, die Gauß selbst anwendet, sind seine Theorie der quadratischen Reste und quadratische Formen. In den letzten Jahrzehnten sind zu den Problemen der Primzahlerkennung und der Faktorzerlegung große Fortschritte erzielt worden, die durch das Aufkommen leistungsstarker Computer ermöglicht wurden. Neben der Fortentwicklung klassischer Methoden wurden dazu auch neue Ideen eingebracht, wie probabilistische Verfahren und die Anwendung der Theorie der elliptischen Kurven über endlichen Körpern.

Neben den traditionellen Inhalten der elementaren Zahlentheorie werden in dem Buch auch die Multiplikation großer ganzer Zahlen mittels der schnellen Fourier-Transformation sowie die Faktorisierung ganzer Zahlen mit elliptischen Kurven und mit der Klassengruppe imaginär-quadratischer Zahlkörper behandelt. In der jetzigen zweiten Auflage sind u.a. eine ausführliche Beschreibung der Faktorisierung

mit dem multipolynomialen quadratischen Sieb sowie Abschnitte über den diskreten Logarithmus und den deterministischen AKS-Primzahltest hinzugekommen.

An mathematischen Vorkenntnissen reicht im Wesentlichen das aus, was man in den Anfänger-Vorlesungen des ersten Studienjahres lernt; insbesondere wird vorausgesetzt, dass der Leser weiß, was eine Gruppe, ein Ring oder ein Körper ist und dass er Begriffe wie Homomorphismus, injektiv und surjektiv kennt. Der zweite Teil des Buches, der ab §16 (quadratische Erweiterungen) beginnt, ist etwas anspruchsvoller als der erste.

Eine Besonderheit dieses Buches ist, dass viele Algorithmen (statt durch Pseudo-Code) mit lauffähigem Code für den PASCAL-ähnlichen Multipräzisions-Interpreter ARIBAS beschrieben werden, der zum kostenlosen Download zur Verfügung steht. Es sind nur geringfügige Programmier-Kenntnisse (in PASCAL, C oder einer ähnlichen Programmiersprache) nötig, um sich mit ARIBAS zurechtzufinden. (Eine Kurzanleitung für ARIBAS steht im Anhang.) Damit kann der Leser die Algorithmen (nicht nur in kleinen Spielbeispielen) sofort auf seinem Laptop oder PC testen und durch das Studium der Quelltexte und die leicht mögliche Abänderung und Anpassung des Codes zu einem vertieften Verständnis gelangen.

Ich danke den vielen sorgfältigen Leserinnen und Lesern der ersten Auflage, durch deren Hilfe zahlreiche Druck- und sonstige Fehler korrigiert werden konnten. Weitere Fehlermeldungen und Kommentare zum Buch oder zum Programm ARIBAS sind willkommen.

München, September 2014 Otto Forster

Bezeichnungen. Es werden die üblichen Bezeichnungen verwendet. Z.B. bezeichnet $\mathbb{N}$ die Menge der natürlichen Zahlen (einschließlich der 0), $\mathbb{Z}$ den Ring der ganzen Zahlen und $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ die Körper der rationalen, reellen und komplexen Zahlen. Für eine Menge M ist $\mathrm{Card}(M)$ oder $\#M$ die Anzahl ihrer Elemente. Zur Beschreibung des Wachstums von Funktionen benutzen wir die Landau-Notation: $O(\varphi(n))$ bezeichnet die Klasse aller Funktionen $f(n)$, so dass mit geeigneten Konstanten $K > 0$ und $n_0 > 0$ gilt $|f(n)| \leqslant K|\varphi(n)|$ für alle $n \geqslant n_0$.

http://www.springer.com/978-3-658-06539-3

Algorithmische Zahlentheorie
Forster, O.
2015, VIII, 314 S. 7 Abb., Softcover
ISBN: 978-3-658-06539-3